



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/647,644	08/25/2003	Mark Eric Obrecht	6002-00602	2528
35690	7590	08/10/2007	EXAMINER	
MEYERTONS, HOOD, KIVLIN, KOWERT & GOETZEL, P.C. P.O. BOX 398 AUSTIN, TX 78767-0398				SHERKAT, AREZOO
ART UNIT		PAPER NUMBER		
2131				
MAIL DATE		DELIVERY MODE		
08/10/2007		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)
	10/647,644	OBRECHT ET AL.
	Examiner	Art Unit
	Arezoo Sherkat	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 08 May 2007.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 105-107, 109-118 and 127-149 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 105-107, 109-118, 127-133, 135, 137, 139, 140, 142, 144-146, 148 and 150 is/are rejected.

7) Claim(s) 134, 136, 138, 141, 143, 147, 149 is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a))

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
5) Notice of Informal Patent Application
6) Other: _____

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5/8/2007 has been entered.

Response to Amendment

This office action is responsive to Applicant's amendment received on 5/8/2007. Claims 105, 107, 115-118, and 127-128 are amended. Claims 1-104, 108, and 119-126 are cancelled. Claims 129-149 are added. Claims 105-107, 109-118, and 127-149 are pending.

Response to Arguments

Applicant's arguments with respect to claims 105-107, 109-118, and 127-149 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

Claims 146-150 are objected to because of the following informalities: claims 146-150 have been misnumbered. For the purpose of examination, starting from the second claim numbered as 146, claims 146-149 have been renumbered to 147-150.

Appropriate correction is required.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 105-107, 109-118, and 127-150 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 54, 56-62, 64-78, 80-94, and 96-101 of U.S. Publication No. 2004/0054917 (Note that the conflicting application has been issued and mailed as of 6/14/2007). Although the

conflicting claims are not identical, they are not patentably distinct from each other because the scope of the claimed invention is substantially the same.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 105-107, 109-118, 127-133, 135, 137, 139-140, 142, 144-146, 148, and 150 are rejected under 35 U.S.C. 102(e) as being anticipated by Kouznetsov, (U.S. Patent No. 6,973,577).

Regarding claims 105, 115, 117, and 127-128, Kouznetsov discloses a computer-implemented method comprising:

selecting an active program on a computer system as code under investigation, wherein at least some of the code associated with the selected active program is running in kernel mode (i.e., wherein code under investigation is each of the incoming system calls 91,92, and 93 generated by the applications 33, 34, and 35 (shown in figure 2)), and executing malicious code detection code (MCDC) on the computer system (i.e., monitor/analyizer 19), wherein the MCDC includes a first and a second plurality of detection routines (i.e., static analyzer 52 and dynamic analyzer 53)(col. 4, lines 47-58), wherein said executing includes:

applying each of the first plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results, weighting each of the first plurality of results to obtain a first score indicative of whether the code under investigation is valid code (i.e., static analyzer 52 performs behavior checking and generates alerts and histograms only if patterns of suspicious events are observed), applying each of the second plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results, weighting each of the second plurality of results to obtain a second score indicative of whether the code under investigation is malicious code (i.e., dynamic analyzer 53 analyzes histograms and identifies behavioral repetitions within the histograms which indicate behavior characteristic of a computer virus/compromise)(col. 4, lines 38-67 and col. 5, lines 1-7); and

using the first and second scores (i.e., the results indicated by static analyzer 52 and dynamic analyzer 53) to determine whether the code under investigation is

malicious code (i.e., computer viruses are self-replicating program code which often carry malicious and sometimes destructive payloads and “malware” can include Trojan horses, hoaxes, and spam mail - col. 1, lines 45-48)(col. 5, lines 18-67 and col. 6, lines 1-30).

Regarding claims 106 and 116, Kouznetsov discloses the method of claim 105, wherein the code under investigation has access to other active programs/code executing on the computer system (i.e., events such as program executions, sending of electronic mail, changing to security settings, impersonations, and etc. are monitored)(col. 5, lines 18-67 and col. 6, lines 1-30).

Regarding claims 107 and 118, Kouznetsov discloses the method of claim 105, further comprising:

selecting one or more additional active programs as code under investigation, and executing said MCDC with respect to said selected code under investigation (col. 4, lines 3-67).

Regarding claims 109-114, Kouznetsov discloses the method of claim 105, wherein the malicious code includes monitoring software (i.e., events such as system calls having the ability to monitor system input/output activities are monitored)(col. 5, lines 18-67 and col. 6, lines 1-30).

Regarding claim 129, Kouzentsov discloses the method of claim 105, further comprising:

determining from the first and second scores that the code under investigation is malicious code (i.e., replication technique, an electronic mail-based computer virus, impersonation, and illicit input/output monitoring activity)(col. 5, lines 43-67 and col. 6, lines 1-30).

Regarding claim 130, Kouzentsov discloses the method of claim 129, wherein the malicious code does not have a known signature (i.e., a knowledge of specific, pre-identified computer viruses would not be necessary because behavioral patterns typical of computer viruses are observed. An example of malicious code with unknown signature is polymorphic viruses)(col. 2, lines 1-2 and lines 21-29).

Regarding claim 131, Kouzentsov discloses the method of claim 105, wherein a signature associated with the code under investigation is not used by the first plurality of detection routines (i.e., static analyzer 52 performs behavior checking and generates alerts and histograms, wherein “behavior checking” is monitoring the occurrence of an event from the events list)(col. 4, lines 47-67 and col. 5, lines 1-6).

Regarding claim 132, Kouzentsov discloses the method of claim 131, wherein a signature associated with the code under investigation is not used by the second plurality of detection routines (i.e., dynamic analyzer 53 analyzes histograms and

identifies behavioral repetitions within the histograms which indicate behavior characteristic of a computer virus, wherein such histograms are not know virus signatures associated with any virus)(col. 4, lines 47-67 and col. 5, lines 1-6).

Regarding claim 133, Kouzentsov discloses the method of claim 105, wherein the first and second plurality of detection routines are not specific to the code under investigation (col. 4, lines 15-37).

Regarding claim 135, Kouzentsov discloses the method of claim 105, further comprising:

determining from the first and second scores that the code under investigation is valid code (i.e., static analyzer 52 performs behavior checking and generates alerts and histograms only if patterns of suspicious events are observed)(col. 4, lines 38-67 and col. 5, lines 1-40).

Regarding claim 137, Kouzentsov discloses the method of claim 105, further comprising:

determining from the first and second scores that the code under investigation is suspicious code, wherein suspicious code has not been determined to be either valid or malicious code (i.e., the observed group of suspicious events could “potentially” be malicious)(col. 4, lines 38-67 and col. 5, lines 1-67 and col. 6, lines 1-30).

Regarding claim 139, Kouzentsov discloses the system of claim 127, further comprising program instructions executable by the processor to:

determine from the first and second scores that the code under investigation is malicious code (i.e., replication technique, an electronic mail-based computer virus, impersonation, and illicit input/output monitoring activity)(col. 5, lines 43-67 and col. 6, lines 1-30).

Regarding claim 140, Kouznetsov discloses the system of claim 139, wherein the malicious code does not have a known signature (i.e., a knowledge of specific, pre-identified computer viruses would not be necessary because behavioral patterns typical of computer viruses are observed. An example of malicious code with unknown signature is polymorphic viruses)(col. 2, lines 1-2 and lines 21-29).

Regarding claim 142, Kouzentsov discloses the system of claim 127, further comprising program instructions executable by the processor to:

determine from the first and second scores that the code under investigation is valid code (i.e., static analyzer 52 performs behavior checking and generates alerts and histograms only if patterns of suspicious events are observed)(col. 4, lines 38-67 and col. 5, lines 1-40).

Regarding claim 144, Kouzentsov discloses the system of claim 127, further comprising program instructions executable by the processor to:

determine from the first and second scores that the code under investigation is suspicious code (col. 4, lines 38-67 and col. 5, lines 1-40).

Regarding claim 145, Kouzentsov discloses the memory medium of claim 128, further comprising program instructions executable to:

determine from the first and second scores that the code under investigation is malicious code (i.e., replication technique, an electronic mail-based computer virus, impersonation, and illicit input/output monitoring activity)(col. 5, lines 43-67 and col. 6, lines 1-30).

Regarding claim 146, Kouzentsov discloses the memory medium of claim 145, wherein the malicious code does not have a known signature (i.e., a knowledge of specific, pre-identified computer viruses would not be necessary because behavioral patterns typical of computer viruses are observed. An example of malicious code with unknown signature is polymorphic viruses)(col. 2, lines 1-2 and lines 21-29).

Regarding claim 148, Kouzentsov discloses the memory medium of claim 128, further comprising program instructions executable to:

determine from the first and second scores that the code under investigation is valid code (i.e., static analyzer 52 performs behavior checking and generates alerts and histograms only if patterns of suspicious events are observed)(col. 4, lines 38-67 and col. 5, lines 1-40).

Regarding claim 150, Kouzentsov discloses the memory medium of claim 128, further comprising program instructions executable to:

determine from the first and second scores that the code under investigation is suspicious code (col. 4, lines 38-67 and col. 5, lines 1-40).

Allowable Subject Matter

Claims 134, 136, 138, 141, 143, 147, and 149 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Please see the attached PTO-892 for a complete listing.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

A.S.
Patent Examiner
Group 2131
July 26, 2007

SYEDA A. SYED
PRIMARY EXAMINER
8/2/2007